Cassandra Crossing/ Rakshasa: dal profondo del tuo hardware

(255)—Nessuna via di scampo al demone mostrato a Defcon. Paranoia? Speculazioni tecniche? Poco importa: le backdoor hardware sono…

Cassandra Crossing/ Rakshasa: dal profondo del tuo hardware

Figure 1:

(255)—Nessuna via di scampo al demone mostrato a Defcon. Paranoia? Speculazioni tecniche? Poco importa: le backdoor hardware sono realizzabili.

14 agosto 2012—Peccato arrivare all'età di Cassandra ed ancora non essere mai riuscito a partecipare ad uno degli eventi storici sulla sicurezza e dintorni come Blackhat o Defcon.

Ma la Rete offre molte possibilità di partecipazione differita che l'agosto aiuta a sfruttare, spigolando tra i soliti nugoli di segnalazioni fino a trovare qualcosa la cui lettura ti gratifichi.

E Cassandra è stata particolarmente lieta di trovarne una che le ricorda tanto la sua giovinezza, quando non riuscì a convincere il babbo che quei risolini provenienti dal cavallo di legno potevano essere di cattivo auspicio.

Ricordandomi di alcuni anni passati nello sviluppo HW di un'azienda che con tutti i suoi difetti era un posto magnifico in cui lavorare, avevo sempre seguito con interesse il livello di intelligenza autonoma e di autoconfigurabilità che i personal computer andavano acquistando, chiedendomi perché che nessun malintenzionato riuscisse a farne uso come vettore di attacco.Un vettore di attacco è la funzionalità principale che viene usata, anzi abusata, per condurre un attacco informatico.

Attacchi molto noti, come nel caso di Stuxnet, usano una o più debolezze di un sistema informatico per installare un rootkit, cioè un software malevolo che può agire con i massimi privilegi senza farsi rilevare dall'utente o da contromisure comuni come un antivirus.

Un rootkit moderno permette poi di installare un payload, di solito un malware, lui pure moderno e modulare, che può permettere qualsiasi attività, da una operazione di intercettazione telematica, la creazione di una botnet od un vero e proprio atto di cyberwar come appunto Stuxnet.

Ma tutto questo era confinato (come se non bastasse) al mondo del software: quando possibile una bella reinstallazione permetteva di sradicare anche la più raffinata delle infezioni.

Ora non più…Dalle profondità del vostro hardware un nero tentacolo potrà risalire fino a voi ed impossessarsi della vostra anima elettronica. Esseri innominabili e deformi, che nemmeno Lovecraft avrebbe potuto immaginare, stanno per occhieggiare dietro le fenditure della ventola.

Raramente capita di veder bene impacchettato in una dozzina di pagine una quantità cosi rilevante e ben assortita di informazioni a supporto di un lavoro emozionante e quasi demoniaco come la proof-of-concept di un malware innovativo.

E molto opportunamente Jonathan Brossard, l'autore di questo lavoro presentato pochi giorni fa a Defcon 20 in quel di Las Vegas, l'ha battezzato Rakshasa, parola hindi che si traduce con "demone".

Il seguito del titolo dice tutto: "Le backdoor hardware sono realizzabili".

Non è qui il caso di accennare come un codice malevolo possa funzionare senza essere presente sul PC e su come possa disabilitare il bit di non esecuzione della memoria o togliere gli aggiornamenti del microcodice delle CPU: queste e ben altre delizie sono, all'uso cassandresco, riservate solo a chi avrà voglia di approfondire la notizia e magari di farne il punto di partenza per un nuovo interesse.

Giusto perché è agosto e si suda, la generosità di Cassandra si spingerà fino a fornirvi un meno accademico e più discorsivo punto di partenza come le slide dell'intervento di Brossard a Defcon.

Per tutti gli altri pigroni invece, solo fosche previsioni e profezie di disgrazie imminenti.

Cosa succederebbe se fosse possibile infettare così profondamente il vostro PC che nemmeno riformattare l'hard disk o addirittura sostituirlo interamente, riflashando anche il BIOS per sovrappiù, permettesse di sradicare l'infezione?E quali possibilità aggiuntive queste tecniche fornirebbero ai creatori di malware, siano essi botnet per la produzione di spam, armi informatiche o raffinatissimi strumenti di intercettazione e tecnocontrollo?

Bene, via i condizionali: chiamatelo come volete, notizia tecnica, incubo, bollettino di guerra o paranoia, ma tutto questo da oggi è possibile.

Buona lettura.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero